МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
Навчально-науковий Інститут комп'ютерних інформаційних технологій
Кафедра комп'ютерних інформаційних технологій

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
Савченко А.С.
"____" лютого 2020 р.

ДИПЛОМНА РОБОТА
(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНА ОСВІТНЬО-КВАЛІФІКАЦІЙНОГО РІВНЯ
"МАГІСТР"

Тема: "Безпроводова MESH-мережа з енергозбереженням та балансуванням мережного навантаження"

Виконала: Станіславова Ольга Олександрівна

Керівник: доц. Малежик Олександр Іванович

Нормоконтролер з ЄСКД (ЄСПД): доц.Райчев Ігор Едуардович

Київ — 2020

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Навчально-науковий Інститут комп'ютерних інформаційних технологій

Кафедра комп'ютерних інформаційних технологій

Освітньо-кваліфікаційний рівень **Магістр**

Напрям (спеціальність) 122 "Інформаційні управляючі системи та технології"

(шифр, найменування)

ЗАТВЕРДЖУЮ

Завідувач кафедри

Савченко А.С.

"14" жовтня 2019 р.

ЗАВДАННЯ

на виконання дипломної роботи студента

Станіславової Ольги Олександрівни

(прізвище, ім'я, по батькові)

1. **Тема роботи**: "Безпроводова MESH-мережа з енергозбереженням та балансуванням мережного навантаження" затверджена наказом ректора від "25" вересня 2019 р. №2175/ст.
2. **Термін виконання роботи**: з 14 жовтня 2019 р. по 9 лютого 2020 р.
3. **Вихідні дані до роботи**: аналіз безпроводової MESH-мережі з подальшою її реалізацію як "розумної" сенсорної мережі на прикладі автоматизації готелю.
4. **Зміст пояснювальної записки** (перелік питань, що підлягають розробці): Ad-hoc – основа Mesh-мережі, Mesh-мережа, сенсорні датчики – технологічні органи відчуття, оптимізація сенсорної мережі, автоматизація за допомогою сенсорної мережі.

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назва етапу дипломного проекту (роботи)	Термін виконання	Примітка
1.	Отримання завдання на дипломну роботу	14.10.2019	
2.	Підбір і вивчення літературних джерел. Обґрунтування необхідності реалізації "розумної" сенсорної мережі на прикладі автоматизації готелю	15.10.2019 – 02.11.2019	
3.	Огляд та аналіз Mesh-мереж та сенсорних датчиків	03.11.2019 – 08.11.2019	
4.	Аналіз необхідних інструментів для розробки сенсорної мережі	09.11.2019 – 23.11.2019	
5.	Вибір оптимального обладнання для реалізації мережі	02.12.2019 – 25.12.2019	
6.	Розробка двох видів реалізації для практичного застосування мережі	08.01.2020– 18.01.2020	
7.	Технічне оформлення пояснювальної записки	19.01.2020 – 25.01.2020	
8.	Підготовка до захисту дипломної роботи.	26.01.2020– 03.02.2020	

Студентка Станіславова Ольга Олександрівна

Керівник дипломної роботи Малежик Олександр Іванович

6. Консультанти з окремих розділів роботи:

Розділ	Консультант (посада, П.І.Б.)	Дата, підпис	
		Завдання видав	Завдання прийняв

7.Дата видачі завдання _____

Керівник _____
(підпис)

Завдання прийняв до виконання _____
(підпис студента)

Дата _____

РЕФЕРАТ

Пояснювальна записка до дипломного проекту: "Безпроводова MESH-мережа з енергозбереженням та балансуванням мережного навантаження" містить 56 сторінок, 10 ілюстрацій, 2 таблиці, 16 формул, 13 джерел літератури.

Ключові слова: MESH-МЕРЕЖА, AD-HOC, WMAN, WLAN, WPAN, BLUETOOTH, ZIGBEE.

Мета дипломного проекту — на основі аналізу та подальшої оптимізації сенсорної мережі, розглянути проблеми, пов’язані з труднощами організації мережі, з метою подальшої реалізації "розумної" сенсорної мережі на прикладі автоматизації готелю.

Завдання дипломного проектування — проаналізувати MESH-мережі, питання їх захищеності і сфери застосування; проаналізувати мережі. Що складаються з сенсорних датчиків, розглянути ієрархію сенсорної мережі, взаємодію вузлів у ній, а також топологію, розповсюдження і поняття спрямованої дифузії; провести оптимізацію сенсорної мережі з подальшою автоматизацією системи готелю з її допомогою.

Об’єкт проектування — безпроводова MESH-мережа.

Практична значимість проекту полягає в створені мережа такого плану, яка можлива для реалізації не тільки в готелі, така система прийнятна і для лікарень, портів, шкіл або будь-яких інших установ.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

MESH — спеціальний, створений для даної мети

Ad-Hoc — для спеціального призначення

WEP — Wired Equivalent Privacy

WPA — Wi-fi Protected Access

TKIP — Temporal Key Integrity Protocol

MIC — Message Integrity Check

WPA-PSK — Pre-shared key

EAP — Extensible Authentication Protocol

TLS — Transport Layer Security

RADIUS — Remote Authentica-tion Dial-in User Server

БСМ — безпроводова сенсорна мережа

ВСТУП

Мініатюризація процесів виробництва мікросхем і прогрес технологій безпроводового зв'язку відкриває нові горизонти застосування інформаційно-комп'ютерних технологій – розвиток сенсорних мереж. Експерти пророкують, що незабаром мільярди мікроскопічних сенсорів, вбудованих майже в усі предмети, що нас оточують, від дерев до дитячих підгузків, зможуть реагувати на зміни в обстановці і взаємодіяти одне з одним, вирішуючи безліч нагальних проблем. Те, що кілька десятиліть тому передбачали письменники-фантасти, вже зовсім скоро стане нашим повсякденним життям. Наближається нова ера - безпроводові сенсорні MESH - мережі.

Умовою ефективної роботи є необхідність об'єднати сенсори в єдину мережу з безлічі вузлів. Дослідникам Intel вдалося створити спеціальні динамічні та самоналагоджувальні мережі, що використовують mote-сенсори з живленням від батарей, які шукають і самостійно встановлюють контакт з сусідніми сенсорами. Коли ці сенсори переміщуються, мережа динамічно змінює конфігурацію. Зараз завдання полягає в тому, щоб зробити датчики дійсно розміром з порошинку (mote).

На одній з публічних демонстрацій такої мережі на Форумі Intel для розробників по всій аудиторії було розкидано більше сотні м'ячів з прикріпленими до них датчиками, а з базової станції запустили серію алгоритмів, які визначали становище кожного датчика і його найближчих датчиків-сусідів. Мережа сама обчислювала оптимальний маршрут проходження даних. На екрані можна було спостерігати, по якому шляху проходять дані. Вузли перенаправляли дані 20-25 разів за секунду протягом приблизно п'яти переміщень м'ячів, при цьому швидкість передачі даних становила 10 Кбіт/с. Для того, щоб самостійно змінити конфігурацію мережі, було потрібно близько 5 секунд. Під час іншої демонстрації була створена найбільша в світі самоналаштовувана мережа, яка складалася з кількох тисяч вузлів. Уявіть, чи зможе оператор всього за кілька секунд сконфігурувати мережу, яка містить хоча б кілька десятків вузлів?

Термін MESH (спеціальний, створений для даної мети) відображує суть подібних сенсорних мереж, які організовуються кожного разу для вирішення конкретних завдань і розпадаються на окремі елементи після їх виконання, готові утворити нові мережі, щойно в цьому виникне необхідність. Крихітні, як «порошинки» (mote), напівпровідникові пристрої, що виконують одночасно обчислювальні та комунікаційні функції і здатні найбільш оптимальним чином автоматично конфігуруватися в самоорганізовувані мережі, і є основою нової парадигми MESH-мереж, що підвищує продуктивність і безпеку мережевих обчислень.

У концепції сенсорних мереж кардинально змінюється роль людини, оскільки їх елементи - сенсорні мікрокомп'ютери - стають набагато більш самостійними, часто передбачають наші дії. «Гомоцентрична» модель мережевих обчислень з людиною в якості центральної ланки в такій новій мережі відходить у минуле - людина перестає бути центром обчислень і стає лише посередником між реальним світом і комп'ютерами, концентруючись на загальній організації системи.

Зрозуміло, щоб втілити в життя привабливі мрії про сенсорні безпроводові мережі, треба ще багато що зробити. Малогабаритні датчики (mote) повинні не тільки інтелектуально відслідковувати стан середовища, самоорганізовуватися в єдину безпроводову мережу і володіти пристойним запасом енергії для автономної роботи, але й діяти залежно від обстановки. І бути при цьому досить дешевими, щоб їх було дешевше викинути, ніж підзарядити. Поширення сенсорних мереж може створити ефект незрівнянно більший, ніж поширення Інтернету.

У рамках магістерської роботі неможливо розглянути досить масштабний проект, тому прикладом та водночас об’єктом дослідження буде невелика сенсорна мережа контролю над готелем. Даний проект буде розглянутий виключно теоретично, хоча практична його реалізація також цілком імовірна.

Одним з центрів розробки сенсорних мереж, координуючим зусилля академічної спільноти та індустрії, є дослідницька лабораторія корпорації Intel в Каліфорнійському університеті, що в Берклі. Головною метою є створення інтегрованої безпроводової обчислювальної платформи-сенсора з низьким енергоспоживанням. Роботи ведуться у трьох основних напрямках: розробка гнучкої і відкритої операційної системи; створення мережевих технологій, що забезпечують самоорганізацію мереж з сенсорів; розробка потрібних програм для mesh-мереж.

РОЗДІЛ 1

AD-HOC – ОСНОВА MESH-МЕРЕЖІ

1.1. Ad-Hoc мережі

Безпроводові Ad-Hoc мережі визнано перспективною технологією радіозв'язку, що підтверджується як вже існуючими застосуваннями, так і увагою з боку науковців. За останні роки було реалізовано ряд промислових проектів з практичного втілення різних типів Ad-Hoc мереж (MANET, mesh networks, sensor networks), опубліковано значну кількість досліджень.

Але ті ж самі принципи, які забезпечують Ad-Hoc мережам ефективність та привабливість, в той же час роблять складною і критичною проблему безпеки. Той рівень гарантій, який може бути забезпечено існуючими механізмами безпеки в Ad-Hoc мережах, не є прийнятним для певних застосувань, в яких існують вищі вимоги щодо передачі інформації з обмеженим доступом або критичної відкритої інформації . Це обмежує можливості широкого застосування даної технології.

1.2. Принципи організації зв'язку в Ad-Hoc мережах

Безпроводові Ad-Hoc (лат. – для спеціального призначення) мережі за принципами організації кардинально відрізняється від традиційних телекомунікацій. Цими принципами є:

- можливість утворення мережі випадковими абонентами;
- децентралізація, відсутність інфраструктури (наприклад, базових станцій);

- багатокрокова (multi-hop) маршрутизація з перенаправленням (forwarding) пакета від вузла до вузла.

Останній принцип має на увазі, що кожен вузол мережі може відігравати роль безпроводового маршрутизатора-посередника (intermediate router), перенаправляючого IP пакети до наступного (next-hop) вузла, який в свою чергу може бути або кінцевим отримувачем (destination) або також посередником.

Головними перевагами Ad-Hoc мереж є:

- можливість оперативного швидкого розгортання;
- мінімальні вимоги, низька вартість пристроїв, відсутність вимог до попередньо існуючої інфраструктури і завдяки цьому низька загальна вартість;
- можливість більшого покриття, масштабованості, живучості.

Хоча Ad-Hoc мережі розроблялися в 70-х роках в першу чергу для задовольняння військових потреб США, зараз їхні переваги роблять їх дуже привабливими і для сучасних невійськових застосувань, таких як:

- зв’язок у надзвичайних ситуаціях (рятівні, антитерористичні операції);
- організація оперативного тимчасового зв’язку між різними типами пристроїв (конференції, виїзні роботи, експерименти);
- дешевий доступ до Інтернет (там де невигідно будувати інфраструктуру);
- місцеві, муніципальні, відомчі, університетські мережі (community networks);
- мережі зв’язку між транспортом , що пересувається(vehicular networks);
- збір та моніторинг даних за допомогою сенсорних мереж: телеметрія, телебіометрія, радіочастотна ідентифікація (RFID).

Вже розпочато розробки з використання Ad-Hoc мереж для самоорганізації зв’язку між нанопристроями (наносенсорами, нанороботами).

На сьогоднішній день Ad-Hoc мережі (за виключенням сенсорних мереж) будуються повністю на базі вже існуючого програмно-апаратного забезпечення, фізичного та канального інтерфейсів в рамках стандартів безпроводового зв’язку, так на (рис.1.1) наведений приклад простої Ad-Hoc мережі. В якості мережного

рівня використовується стандартний стек інтернет-протоколів, в останній час його остання версія IPv6, спеціально розроблена з врахуванням потреб мобільних пристроїв та безпеки. Транспортний рівень також зазвичай не відрізняється від стандартного стеку TCP/IP і використовує TCP та UDP.

Як правило для переключення мережі в режим Ad-Hoc достатньо лише встановити в системних настройках клієнтського програмного забезпечення (драйвер безпроводового мережного адаптеру) опцію роботи в режимі одноранговоі мережі (Ad-Hoc). Таким чином можна створити клієнтську Ad-Hoc мережу або MANET (Mobile Ad-Hoc Network), з'єднавши портативні комп'ютери (ноутбуки), КПК, PDA, комунікатори, мобільні телефони або інші мобільні пристрої, в яких присутні адаптери стандартних фізичних та канальних інтерфейсів IEEE 802.11 (Wi-Fi) або IEEE 802.15.1 (Bluetooth).

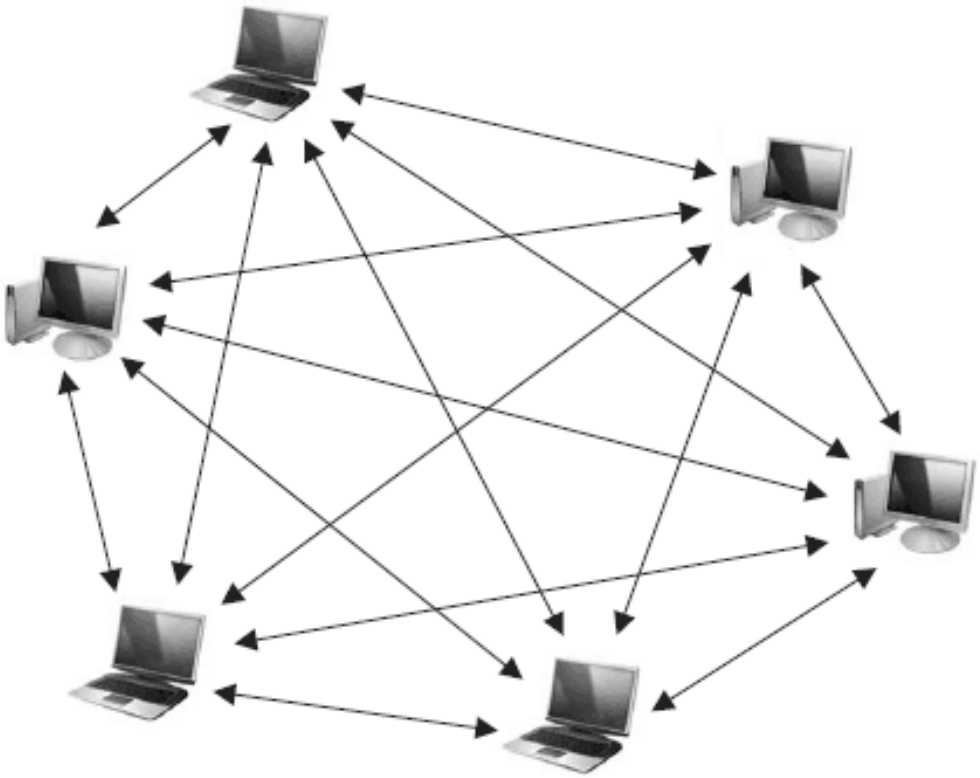

Рис. 1.1 – приклад Ad-Hoc мережі

Також за принципом Ad-Hoc мережі організується зв'язок між сенсорами, які збирають та передають дані моніторингу фізичних параметрів навколишнього середовища (акустичних, оптичних, інфрачервоних, тиску, температурних,

радіочастотних тощо) або параметрів біологічних організмів, зокрема людини (телебіометрія). В сенсорних мережах в якості фізичного та канального інтерфейсів використовується спеціально розроблений стандарт ZigBee. Самі сенсори працюють під керуванням операційної системи TinyOS.

Принцип організації зв'язку в Mesh мережах хоча і наслідує більшість підходів Ad-Hoc мереж, однак спирається на інфраструктуру у вигляді безпроводових стаціонарних маршрутизаторів (Mesh-роутерів), які відіграють роль точок безпроводового доступу з певним обмеженим радіусом дії. Mesh-роутери не підключаються до фіксованої мережі (як традиційні точки доступу Wi-Fi), а натомість з'єднані один з одним за допомогою безпроводового зв'язку за принципом Ad-Hoc мережі, тобто пересилають пакети через радіоканали від одного роутера до іншого.

1.3. Складності в забезпеченні захисту інформації

Однак принципи організації Ad-Hoc мереж зумовлюють також і складність забезпечення захисту інформації, через такі причини:

- відкритість середи передачі;
- незахищеність та можливість компрометації вузлів;
- вразливості маршрутизації пакетів;
- розподіленість та децентралізованість з відсутністю інфраструктури;
- вразливості зумовлені динамічністю змін у топології та мобільністю;
- вразливості протоколів через помилки або надмірну складність;
- технічні обмеження (простота обладнання, полоса пропускання).

Незахищеність радіоефіру як відкритої середи передачі надає порушнику можливості прослуховування, зашумлення каналів зв'язку, закладання або модифікації пакетів. Ця проблема є спільною для всіх безпроводових мереж і вирішується зазвичай на різних рівнях моделі OSI:

- на мережному рівні (IPv6): VPN; IPSec з криптографічним шифруванням пакетів з використанням блочних симетричних алгоритмів (3DES, AES-128, ГОСТ 28147) та контролю цілісності пакета шляхом розрахунку значення імітовставки HMAC на основі значень геш-функцій SHA-1 або MD5;
- на канальному рівні: шифрування потоковими симетричними криптоалгоритмами інформації, що передається через відкритий канал радіозв'язку (RC4, CCMP RFC2610); застосування широкосмугового сигналу, завадостійке та помилкокорегуюче кодування, геш-функція CRC32;на фізичному рівні: направленими антенами та контролем меж розповсюдження радіосигналу.Однак у випадку Ad-Hoc мереж використання вказаних заходів ускладнене. Навіть якщо в тій мірі, в якій це дозволяє децентралізована динамічна топологія, використовувати механізми безпеки, які запропоновані в базових стандартах (наприклад IEEE 802.11.i), все одно залишаються критичні вразливості, які дуже важко перекрити.

Зокрема, криптографічні засоби повинні спиратися на механізми розподілу ключів, такі як інфраструктура відкритих ключів (PKI) з сервером сертифікатів ключів. Однак, в багатьох випадках Ad-Hoc мережі повністю децентралізовані та не мають постійної інфраструктури, тому використання центральних серверів може бути неможливе. Навіть якщо є певна централізована структура (захищений сервер), все одно існує можливість компрометації незахищених вузлів мережі та отримання таким чином несанкціонованого доступу до ключової інформації. Крім того, можливість відносно легкої компрометації вузла (наприклад, шляхом фізичного доступу) створює додаткові внутрішні загрози, так звані Візантійські атаки (Byzantine attacks). В зв'язку з цим виникає ситуація, коли не можливо довіряти будь-якому внутрішньому вузлу, який може бути інсайдером (Byzantine attacker), тобто авторизованим вузлом, який має аутентифікаційну інформацію (ключі) і є «легалізованим» учасником інформаційного обміну.

Як можна побачити, навіть механізми шифрування, контролю цілісності, розподілу ключів та керування доступом шляхом аутентифікації не вирішують

повністю проблему безпеки Ad-Hoc мереж. Ще більше загострює проблему той факт, що будь-який (навіть компрометований) вузол мережі потенційно може відігравати роль маршрутизатора, який повинен пересилати пакети, призначені іншим вузлам. В зв’язку з легкістю компрометації будь-якої кількості таких маршрутизаторів, та вразливістю існуючих протоколів маршрутизації в Ad-Hoc мережах виникає безліч можливостей для реалізації Візантійських атак як на рівні контролю (control plane), так і на рівні даних (data plane, forwarding) маршрутизації.

Специфіка Ad-Hoc мереж, наявність в них великої кількості вразливостей та неминуча поява інцидентів безпеки призводять до необхідності створювати другий рубіж захисту, який має складатися з реактивних технологій безпеки . Реактивні технології безпеки мають спиратися на механізми виявлення вторгнень та адаптивно реагувати на інциденти шляхом реконфігурації мережної інфраструктури.

ВИСНОВКИ ДО РОЗДІЛУ 1

У ході опрацювання інформації до даного розділу, був розглянутий ряд необхідних при дослідженні тем. У першому розділі це основні аспекти роботи Ad-Hoc мережі, її модель, коротко згадали про її переваги та недоліки.

У другому пункті розділу було детально розглянуто принципи організації зв'язку в Ad-Hoc мережах, розгорнуто описані всі її переваги, наведено декілька способів їх невійськового застосування, а також наглядно проілюстровано приклад Ad-Hoc мережі на рисунку.

Третій пункт був присвячений розгляду питання щодо складності в забезпеченні захисту інформації у Ad-Hoc мережі. Розглянуто та проаналізовано через які саме причини принципи організації Ad-Hoc мереж зумовлюють також і складність забезпечення захисту інформації.

РОЗДІЛ 2

MESH-МЕРЕЖА

2.1. Основні поняття

На теперішній час не існує точних критеріїв, що можуть визначити термін "Mesh-мережа" при застосуванні до систем широкосмугового безпроводового доступу. Найбільш загальне визначення звучить наступним чином: "Mesh-мережева топологія, в якій пристрої об'єднуються багаточисленними (часто надмірними) з'єднаннями, що вводяться із стратегічних міркувань". Mesh-мережа – це багатокрокова мережа, пристрої якої (Mesh-станції, MP, Mesh-Points) володіють функціями маршрутизатора і здатні використовувати різні шляхи для пересилки пакету. В першу чергу поняття Mesh визначає принцип побудови мережі (класифікація MESH-мереж наведена у таблиці 1.1), відмінною особливістю якої є архітектура, що самоорганізується, і реалізує наступні можливості:

- Створення зон єдиного інформаційного покриття великої площі;
- Гнучкість мережі (збільшення площі зони покриття та густоти інформаційного забезпечення) в режимі самоорганізації;
- використання беспроводових транспортних каналів (backhaul) для зв'язку точок доступу в режимі "кожний с кожним";
- витривалість мережі до втрат окремих елементів.

Таблиця 1.1 – Класифікація стандартів фізичних та канальних інтерфейсів MESH-мереж

Тип MESH-мережі	Клас безпроводової технології	Стандарт	Радіус
Mesh Networks	Wireless Metropolitan Area Networks (WMAN)	IEEE 802.16 (Wi-MAX)	декілька км
MANET; Mesh Networks	Wireless Local Area Networks (WLAN)	IEEE 802.11 (Wi-Fi)	~100м – 1км
MANET	Wireless Personal Area Networks (WPAN)	802.15.1 (Bluetooth);	~10м
Sensor Networks		802.15.4a (ZigBee);	

Mesh-мережі будуються як сукупність кластерів. Територія покриття розділяється на кластерні зони, кількість яких теоретично необмежена. Особливістю Mesh-мереж є використання спеціальних протоколів, що дозволяють кожній крапці доступу створювати таблиці абонентів мережі з контролем стану транспортного каналу і підтримкою динамічної маршрутизації трафіку з оптимальним маршрутом між сусідніми станціями.

При відмові будь-якої з них відбувається автоматичне перенаправлення трафіку по іншому маршруту, що гарантує отримання трафіка адресату за мінімальний час. Кожен абонент оснащений радіоустаткуванням для зв’язку з Mesh-маршрутизатором. Завдяки своїм особливостям Mesh-мережі можуть використовуватись в різних сферах.

Основна відмінність Mesh-мережі від архітектури «крапка-багатокрапка» в тому, що якщо в останньому випадку АС може спілкуватися тільки з БС, то в Mesh-мережі можлива взаємодія безпосередньо між АС. Оскільки мережі стандарту IEEE 802.16 орієнтовані на роботу з широкими частотними каналами, Mesh-мережі увійшли до стандарту зовсім не з метою створення однорангових локальних мереж – для цього є стандарти групи IEEE 802.11. Причина в іншому:

необхідний інструмент побудови широкосмугової мережі, в якій трафік може передаватися по ланцюжку з декількох станцій, ліквідовуючи тим самим проблеми передачі за відсутності прямої видимості. Відповідно і всі механізми управління, що у принципі дозволяють побудувати децентралізовану розподілену мережу, орієнтовані все ж таки на деревовидну архітектуру, з виділеною базовою станцією (кореневий вузол) і домінуючими потоками БС-АС.

В Mesh-мережі всі станції (вузли) формально рівноправні. Проте практично завжди обмін трафіку Mesh-мережі із зовнішнім оточенням відбувається через один певний вузол (рис. 2.1). Такий вузол називають базовою станцією Mesh-мережі: саме на нього покладається частина необхідних для управління Mesh-мережею функцій. При цьому управління доступом може відбуватися або на основі механізму розподіленого управління, або централізованим способом під управлінням БС. Можлива і комбінація цих методів.

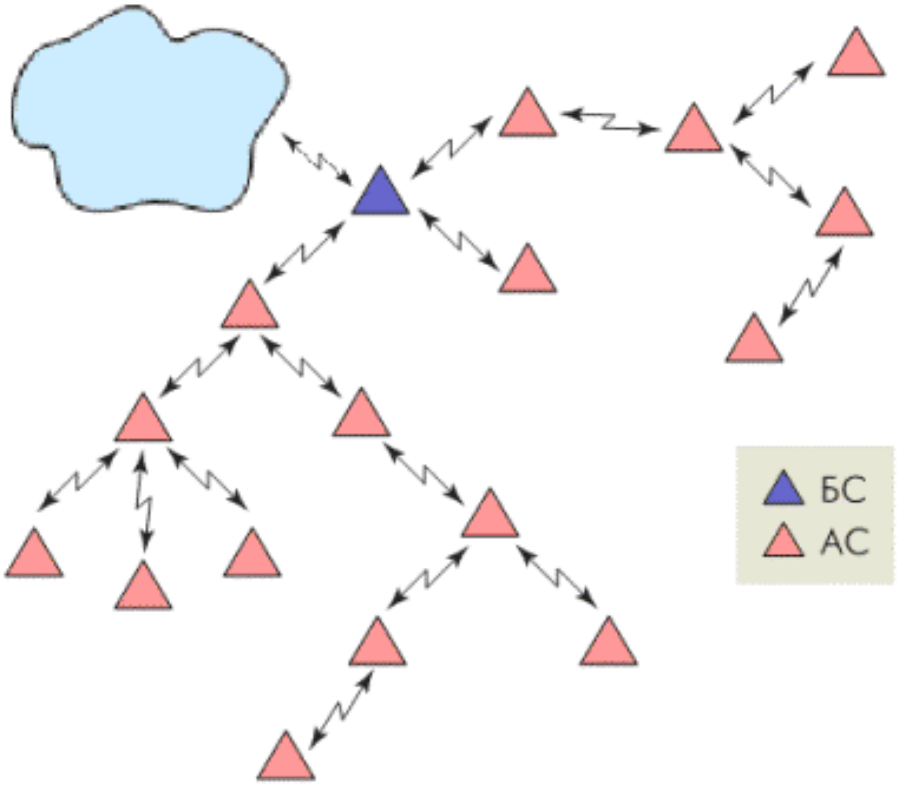

Рис. 2.1. Приклад Mesh-мережі

Базове поняття в Mesh-мережі – сусіди. Під сусідами певного вузла розуміють всі вузли, які можуть встановлювати з ним безпосереднє з'єднання. Всі вони утворюють сусідське оточення. Вузли, пов'язані із заданим вузлом через сусідські вузли, називають сусідами другого порядку. Можуть бути сусіди третього порядку і т.д.

Ранні прототипи сенсорів використовували мікропотужний мікроконтроллер з частотою 4 МГц, 16 Кбайт флеш-пам'яті для інструкцій, 512 байт статичної RAM, кількома АЦП і примітивними периферійними інтерфейсами, а також 256 Мбайт перезаписуємої пам'яті в якості вторинного пристрою збереження. Сенсори, «актуатори» і радіочастотна мережа обслуговувалися як підсистема вводу-виводу. Вузли мережі використовували специфічну операційну систему TinyOS, що займає всього від кілька сотень байт до пари кілобайт. Нині технології помітно пішли вперед і вже створюються кремнієві сенсори об'ємом близько 1 куб. мм, що стане справжнім проривом. Беззаперечним доказом цього є представлений на (рис. 2.2) зразок одного з сенсорних чипів.

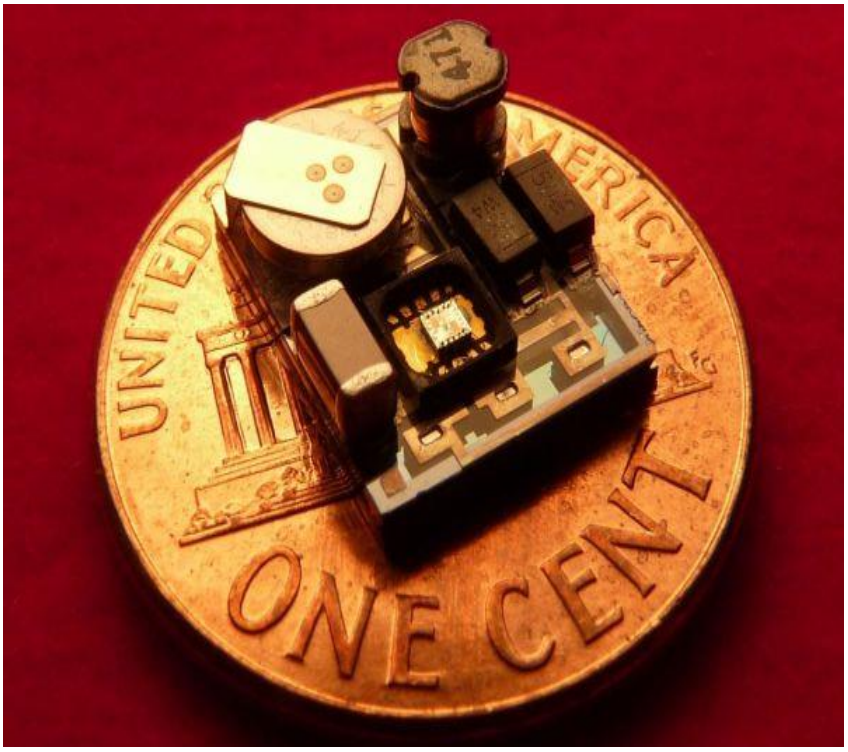

Рис. 2.2. Сенсор у порівнянні з 1 центом США

Пріоритетні напрямки розробок: створення різноманітних актуаторів, біочипів (для аналізу рідких середовищ та їх складу), сенсорів рідких середовищ і об'єктів, що біологічно розвиваються, а також методика об'єднання сенсорів з предметами, моніторинг яких «ставиться» їм у обов'язок. Подібні дослідження відкривають колосальні перспективи для медичних і фармацевтичних розробок, здійснення хімічних процесів і виготовлення біологічних препаратів. Сенсори температури, вологості, атмосферного тиску та інфрачервоного випромінювання дозволять вченим без втручання ззовні стежити за станом живої природи та навколишнього середовища різноманітних організмів в природних умовах. Дані екологічних спостережень передаються по супутниковому каналу в Інтернет, звідки дослідники завантажують їх у режимі реального часу. Технологія сенсорних мереж – це нове слово у спостереженні за станом навколишнього середовища зі значно меншим на неї впливом в порівнянні з втручанням людини.

Методика використання сенсорних мереж буде дуже сильно відрізнятися від нинішніх інтерактивних обчислень, коли або комп'ютери чекають наших вказівок, або ми чекаємо від них результатів. У світі активних обчислень комп'ютери будуть діяти на передньому краї, буквально передбачаючи і передчуваючи всі наші побажання, а іноді навіть діючи від нашого імені на випередження. Треба серйозно задуматися про той час, коли на кожну людину на Землі буде припадати не один, а сто чи навіть тисяча комп'ютерів. При цьому людина буде не центром всього цього обчислювального різноманіття, а деякою «вершиною піраміди», що забезпечує інформаційну взаємодію між комп'ютером і реальним світом, вважає Девід Тенненхауз, віце-президент підрозділу Corporate Technology Group корпорації Intel. Експерти прогнозують швидке настання нової ери так званих проактивних (превентивних, запобіжних) обчислень, коли комп'ютери будуть прямо пов'язані з фізичним світом, зможуть вгадувати бажання людей і навіть діяти на власний розсуд - природно, у відповідності із закладеними в них програмами.

2.2. Питання захищеності MESH-мережі

Питання захисту інформації є одним із найбільш актуальних та проблемних. Тому перевагою безпроводових радіомереж можна вважати різноманітність технологій на яких реалізовується мережа. У залежності від сфери використання мережі та її функціональної потребі, користувач може самостійно обрати і спосіб захисту своєї мережі, таким чином, наприклад у технології Wi-Fi (захист якої, є найбільш значимим) є декілька типів захисту:

1. Технологія WEP (Wired Equivalent Privacy) була розроблена спеціально для шифрування потоку передаваних даних в рамках локальної мережі. Існує 64-, 128-, 256- і 512-бітове шифрування. Для посилення захисту частина ключа є статичною, а інша частина – динамічною.

2. WPA (Wi-fi Protected Access) – стійкіший алгоритм шифрування, ніж WEP. Високий рівень безпеки досягається за рахунок використання протоколів TKIP і MIC.

3. TKIP – протокол інтеграції тимчасового ключа (Temporal Key Integrity Protocol) – кожному пристрою привласнюється змінний ключ.

4. MIC – технологія перевірки цілісності повідомлень (Message Integrity Check) – захищає від перехоплення пакетів і їх перенаправлення. Стандарт TKIP використовує автоматично підібрані 128-бітові ключі, які створюються непередбачуваним способом, і загальне число їх варіацій досягає 500 мільярдів. Складна ієрархічна система алгоритму підбору ключів і динамічна їх заміна через кожних 10 КВ (10 тис. передаваних пакетів) роблять систему максимально захищеною. MIC використовує вельми непростий математичний алгоритм, який дозволяє звіряти відправлені в одній і отримані в іншій крапці дані. Якщо відмічені зміни і результат порівняння не сходиться, такі дані вважаються за помилкові і викидаються. Існують два види WPA.

5. WPA-PSK (Pre-shared key) – для генерації ключів мережі і для входу в мережу використовується ключова фраза. Оптимальний варіант для домашньої або невеликої офісної мережі. Wpa-802.1x – вхід в мережу здійснюється через сервер аутентифікації. Оптимально для мережі крупної компанії.

6. Wpa2 багато в чому побудований на основі попередньої версії, WPA, що використовує елементи IEEE 802.11i. Стандарт передбачає застосування шифрування AES, аутентифікації 802.1x, а також захисних специфікацій RSN і CCMP. Як передбачається, Wpa2 повинен істотно підвищити захищеність Wi-Fi-мереж в порівнянні з колишніми технологіями. По аналогії з WPA, Wpa2 також ділиться на два типи: Wpa2-psk і Wpa2-802.1x.

7. IEEE 802.1x – це порівняно новий стандарт, за основу якого взято виправлення недоліків технологій безпеки, вживаних в 802.11, зокрема можливість злому WEP, залежність від технологій виробника і так далі, 802.1x передбачає підключення до мережі навіть PDA-устройств, що дозволяє вигідніше використовувати саму ідею безпровідного зв'язку. З іншого боку, 802.1x і 802.11 є сумісними стандартами. 802.1x базується на наступних протоколах:

EAP (Extensible Authentication Protocol). Протокол розширеної аутентифікації. Використовується спільно з RADIUS-сервером в крупних мережах.

TLS (Transport Layer Security). Протокол, який забезпечує цілісність і шифрування передаваних даних між сервером і клієнтом, їх взаємну аутентифікацію, запобігаючи перехопленню і підміні повідомлень.

RADIUS (Remote Authentica-tion Dial-in User Server). Сервер аутентифікації користувачів по логіну і паролю. Також з'явилася нова організація роботи клієнтів мережі. Після того, як користувач пройшов етап аутентифікації, йому висилається секретний ключ в зашифрованому вигляді на певний незначний час – термін сеансу, що діє на даний момент. Після його завершення генерується новий ключ і знову висилається користувачеві. Протокол захисту транспортного рівня TLS

забезпечує взаємну аутентифікацію і цілісність передачі даних. Всі ключі є 128-розрядними за умовчанням.

А такі технології, як Bluetooth або ZigBee, використовують принципи попередньої аутентифікації з використання кодованих ключів доступу. Отже захист мережі залежить від обраної технології реалізації мережі.

2.3. Сфери застосування MESH-мереж

Mesh – мережа рішення що найбільш підходить для використання в умовах міста. Вона має високі якості надійності і доступності з'єднання, потенціал цієї технології дає можливість швидко і недорого надавати мобільним користувачам широкосмуговий доступ до ресурсів. Розгортання Mesh – мереж може коштувати набагато дешевше, ніж традиційні дротяні мережі, оскільки вони не вимагають дорогої інфраструктури і прокладки кабелів і, окрім цього, економна в експлуатації, оскільки, як вже наголошувалося, здатна самовідновлюватись і само адаптуватись. В ній відсутній такий недолік як ефект "шийки пляшки", що є досить високим мінусом інших технологій. Також до плюсів можна віднести досить високу надійність даної мережі: у випадку виходу одного з її вузлів, навантаження в даній ситуації розподіляється на сусідні (при правильному проектуванні).

Подібні рішення підходять не тільки для міст, але і для університетів. Наприклад, в даний час компанія Nortel, що належить до числа активістів упровадження Mesh-мереж, працює з одним з університетів США, який, використовуючи її технології, планує запустити мережу Wireless Mesh, покликану забезпечити викладацькому складу і студентам захищене широкосмугове підключення усередині приміщень і на вулиці.

ВИСНОВКИ ДО РОЗДІЛУ 2

Під час написання даного розділу були розглянуті наступні теми: основні поняття MESH-мережі, питання її захищеності, а також сфери застосування.

На основі розглянутої у розділі інформації, можна зробити такі висновки:

методика використання сенсорних мереж буде дуже сильно відрізнятися від нинішніх інтерактивних обчислень, коли або комп'ютери чекають наших вказівок, або ми чекаємо від них результатів;

в залежності від сфери використання мережі та її функціональної потребі, користувач може самостійно обрати і спосіб захисту своєї мережі;

розгортання Mesh – мереж може коштувати набагато дешевше, ніж традиційні дротяні мережі, оскільки вони не вимагають дорогої інфраструктури і прокладки кабелів і, окрім цього, економна в експлуатації, оскільки, як вже наголошувалося, здатна самовідновлюватись і само адаптуватись.

РОЗДІЛ 3

СЕНСОРНІ ДАТЧИКИ – ТЕХНОЛОГІЧНІ ОРГАНИ ВІДЧУТТЯ

3.1. Ієрархія сенсорної мережі

Безпроводова сенсорна мережа (БСМ) може налічувати десятки та сотні безпроводових вузлів, оснащених датчиками.

На першому рівні ієрархії розташовуються сенсорні вузли БСМ, основна задача яких стоїть у зборі локальної інформації про контрольований процес в зоні розміщення агенту. Крім того, вони здатні виконувати наступні функції:

- передача даних у вихідному вигляді вузлам другого рівня ієрархії для аналізу стану контролюємого об’єкта;
- збір даних про власні доступні ресурси и, при необхідності, відправка їх вузлам другого рівня (самодіагностика);
- при втраті зв’язку з координатором мережі, в порядку пріоритету, самостійне виконання функцій тимчасового координатора і створення мережі, в якій накопичуються дані моніторингу;
- по запиту із центру моніторингу, відстеження аномальних явищ та сигналізація про їх появу;
- прийом даних від вузлів другого рівня ієрархії (мобільний агент-координатор).

Другий рівень ієрархії представлений координатором мережі, основою якого є агент керування (мобільний агент-керування). Він виконує наступні функції:

- підтримка роботи субмережі;
- створення деяких еталонних моделей стану на основі зібраних з датчиків даних та відправлення їх по запиту на сенсорні вузли центру моніторингу;
- при відсутності власної субмережі, заміна, у порядку пріоритету, координатора, що вийшов з ладу;
- зміна пріоритетів сенсорних вузлів у залежності від доступних йому внутрішніх ресурсів. Це запобігає появі ситуацій в яких при втраті зв'язку координатора з субмережею, керування на себе візьме вузол з недостатнім внутрішнім ресурсом;
- активізація агентів контролю сенсорних вузлів за запитом, що надійшов з центру моніторингу.

Агенти найвищого рівня вирішують задачі, що пов'язані безпосереднім прийняттям діагностичних и керівних рішень.

3.2. Взаємодія вузлів – поняття колективного керування

Організація мультиагентної взаємодії в групах сенсорів базується на принципах колективного керування.

Основні принципи колективного керування:

- кожний член колективу групи самостійно формує своє керування (визначає свої дії) у поточній ситуації;
- формування керування (вибір дій) кожним членом колективу здійснюється виключно на основі інформації про колективну мету, яка стоїть перед групою, ситуації у середовищі у попередній відрізок та даний момент часу, своєму теперішньому стані та теперішніх діях інших членів колективу;
- в якості оптимального керування (дія) кожного члену колективу в певній ситуації, розуміється таке керування (дія), яке дає максимально можливий внесок у досягненні загальної (колективної) мети;

- оптимальне керування реалізується потягом найближчого відрізку часу у майбутньому, після чого, визначається нове керування.

Колективне керування по своїй концепції завжди децентралізоване. Тому запропонований метод керування сенсорною мережею є найбільш ефективним при реалізації у розподілених мультиагентних системах. Мобільні агенти в умовах безпроводових сенсорних мереж можуть динамічно адаптуватись до змінного інформаційного середовища, працювати автономно, у випадку розриву зв'язку з координатором мережі, а при відновленні з'єднання передавати йому всю накопичену інформацію.

Метод колективного управління та ітераційної процедури оптимізації колективних дій є основою великого числа алгоритмів, призначених для рішення широкого класу задач мультиагентної управління складними технічними системами. Основною відмінністю підходу, що базується на принципах колективного мультиагентної управління, є відносно низька обчислювальна складність алгоритмів. Це дозволяє швидко приймати рішення, близькі до оптимальних, в умовах апріорної невизначеності і ситуації, що змінюється випадково.

3.3. Топологія сенсорної мережі

Топологія сенсорних мереж може приймати будь-який вигляд. В залежності від обраної користувачем чи реалізатором мережі технології керування, тобто якщо мережа створена на основі Bluetooth, то топологія буде або «точка-точка»,або «точка-многоточка», а, наприклад, технологія ZigBee, наочне зображення якої показане на (рис.3.1), має підтримку всіх типів топологій («точка-точка», «зірка»,«дерево», «чарункова мережа»).

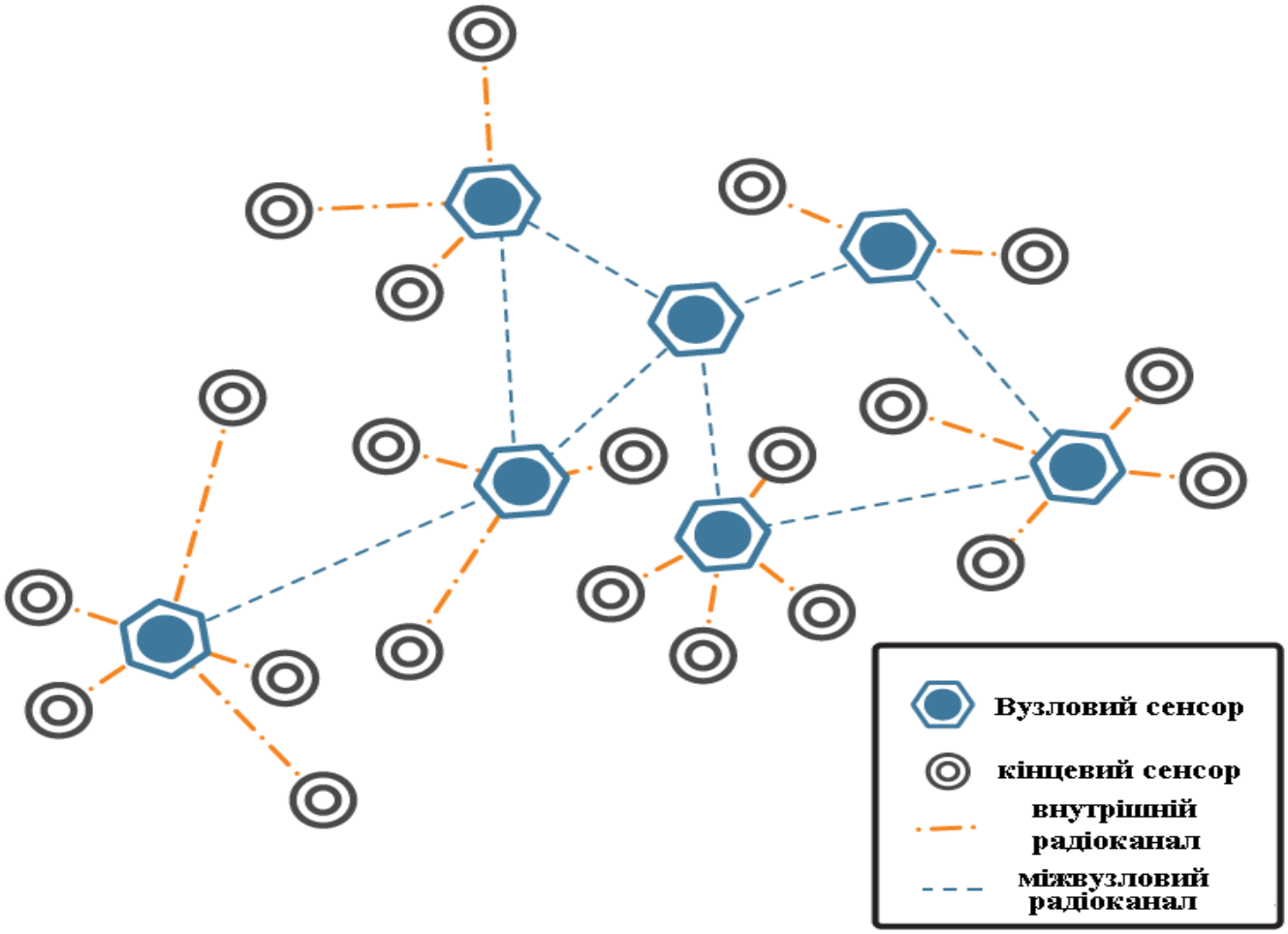

Рис. 3.1. Мережева топологія на основі технології ZigBee

3.4. Поняття спрямованої дифузії

"Спрямована дифузія" (directed diffusion) - ще один термін комп'ютерної новомови, який виник у зв'язку з дослідження сенсорних мереж. За ним стоїть і парадигма, і заснована на ній реалізація мережевих протоколів кожної "пилинки". Уявімо собі, що "порошинки" якимось чином "встановлені" на тваринах - мешканцях національного парку або заповідника. Кожна "порошинка" містить унікальний ідентифікаційний код тварини і, природно, спеціальне програмне забезпечення. Тварини вільно переміщуються в межах заповідника і при цьому утворюють мережу з "порошинок", що має здатність відповідати на запити типу "Скільки хижаків знаходиться в квадраті X?", "Які зміни популяції оленів за останні 6 місяців?" та ін.. Тут варто зауважити, що такою здатністю володіє сама

мережа – не надбудови над нею у вигляді спеціалізованих баз даних, не аналітичні програми, а саме "порох".

Для досягнення такої здатності, очевидно, необхідний механізм комунікації, що радикально відрізняється від практично всіх відомих і поширених. Основу такого механізму - "спрямованої дифузії" - становить принцип адресації, у якому замість адреси одержувача використовується власне ... постановка задачі (така "адреса" в термінах сенсорних мереж називається "інтересом") і принцип багатошляхового розповсюдження (дифузії) "інтересів" мережею "порошинок".

3.5 Радіус розповсюдження мереж

Одним із основних питань при організації безпроводової мережі завжди було і найближчим часом буде, питання про територію, яку та чи інша мережа зможе забезпечити зв’язком. На (рис.3.2) можна побачити характеристику дальності дії мережі того чи іншого протоколу. Таким чином наведені технології займають своє місце у відповідних областях застосування.

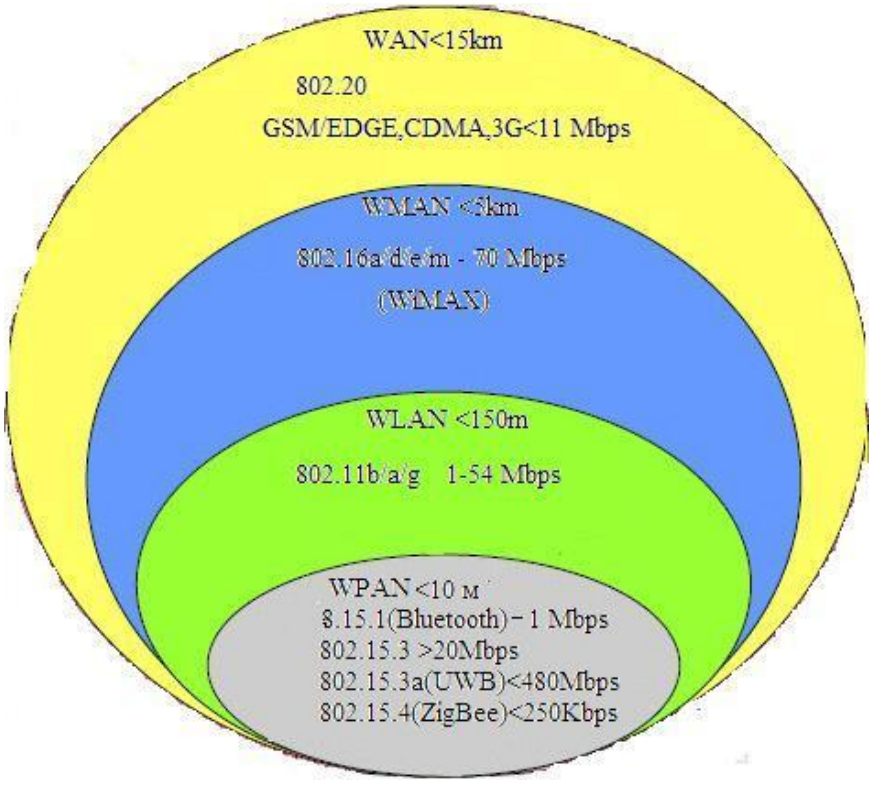

Рис. 3.2. Протоколи, що використовуються в мережах різної дальності дії

Теоретично при реалізації та використанні сенсорних мереж питання дальності не відіграє першочергову роль. Оскільки ціна одного датчика помітно низька, ми можемо використовувати досить велику кількість сенсорів, а оскільки принцип організації мережі дозволяє з’єднання їх як паралельно так і послідовно, сенсорами можна вкрити не тільки лікарню чи будь-який інший об’єкт, а навіть район чи місто. Отже чим більше сенсорних датчиків використовується, тим більша може бути територія покриття. Звісно швидкість розповсюдження даних, збереження їхньої цілісності, швидкість відгуку тих чи інших сенсорів буде під загрозою але теоретично така мережа може існувати.

ВИСНОВКИ ДО РОЗДІЛУ 3

Під час написання даного розділу був проведений детальний розгляд та аналіз мережі з використанням сенсорних датчиків.

Важливим кроком для подальшої роботи є опрацювання питання топології сенсорних мереж, яка може приймати будь-який вигляд в залежності від обраної користувачем чи реалізатором мережі технології керування, а також радіусу її розповсюдження. Чим більше сенсорних датчиків використовується, тим більша може бути територія покриття. Звісно швидкість розповсюдження даних, збереження їхньої цілісності, швидкість відгуку тих чи інших сенсорів буде під загрозою але теоретично така мережа може існувати.

РОЗДІЛ 4

ОПТИМІЗАЦІЯ СЕНСОРНОЇ МЕРЕЖІ

Останніми роками зростає інтерес розгортання мереж радіо датчиків (сенсорних мереж) для вирішення задач розподіленого зондування, збору та обробки даних. На відміну від мереж зв'язку, що базуються на протоколі IP та працюють з глобальною адресацією та маршрутизацією метрики переходів, у сенсорних вузлах, як правило, глобальні адреси відсутні. Також, оскільки мережі після розгортання не обслуговуються, має місце обмеженість у часі функціонування (через низький заряд батареї).

В силу цих особливостей, сенсорні мережі потребують особливої уваги в питанні мінімізації енергоспоживання на більшості рівнів стека протоколів. Для рішення цієї задачі більшість досліджень концентруються на подовженні часу життя мережі, забезпеченні розташування більшої кількості сенсорних вузлів , підвищення стійкості до відмов (наприклад, стійкість до помилок сенсорів чи розряду джерела) Одним з перспективних напрямів досягнення поставленої мети є запровадження механізму спрямованої дифузії і мобільних агентів. У даній роботі проведено аналіз методів маршрутизації в мережі радіодатчиків із застосуванням механізмів спрямованої дифузії.

4.1. Постановка задачі

Більшість енергозберігаючих пропозицій базуються на традиційній клієнт-серверної моделі, коли кожен сенсорний вузол відсилає зібрані дані в центр обробки або вузол збору.

Оскільки ширина каналу безпроводового сенсорної мережі, як правило, набагато нижче, ніж у провідної мережі, трафік даних сенсорної мережі може перевищити можливості мережі. Щоб вирішити проблему перевантаження мережі, була запропонована розподілена сенсорна мережа, заснована на так званих «мобільних агентах» для масштабованого та енергозберігаючого збору даних (цей процес збору називається спільною обробкою сигналів і даних). При передачі програмного коду, що називається «мобільним агентом» (МА), до сенсорних вузлів, велика кількість даних може бути зменшено або перетворено в дані малого обсягу з допомогою ліквідації надмірності. Наприклад, дані сенсорів двох близько розташованих вузлів напевно мають схожі або однакові фрагменти, де дані двох сенсорів повторюються. Тому усунення надмірності при зборі даних є важливою функцією «щільних» сенсорних мереж, що служить для зменшення трафіку даних.

При цьому функціонування мережі ґрунтується на наступних припущеннях:

1. Архітектура сенсорної мережі побудована на кластеризації.

2. Вузли-джерела даних розташовані на відстані одного переходу від вершини кластера.

3. Велика частина надмірності виникає у даних, які можуть бути об'єднані в один пакет даних з фіксованим розміром.

Ці припущення значно обмежують сферу застосування. Дане обмеження механізму кластеризації може бути усунено шляхом вибору плоскої архітектури сенсорної мережі, яка підходить для великої кількості завдань. У такому випадку, необхідно дати відповідь на наступні питання:

- Як ефективно здійснювати маршрутизацію МА від приймача до джерела, від джерела до джерела, і від джерела до приймача?
- Як МА визначає послідовність відвідування декількох вузлів-джерел?
- Якщо дані всіх вузлів-джерел неможливо помістити в один пакет даних з фіксованим розміром, чи буде модель МА ефективніше клієнт-серверної моделі,

наприклад, у разі середовища, в якому вузли розташовані далеко один від одного і дані сенсорів не володіють достатньою надмірністю?

У даній роботі розглядається механізм спрямованої дифузії (СД) для маршрутизації з мобільними агентами (СДМА). СД - це протокол поширення даних в сенсорних мережах, який забезпечує наступні механізми: (а) посилку запитів від вузла збору до потрібних сенсорів, (б) формування градієнтів для надсилання даних від проміжних вузлів до вузла збору. СД забезпечує ефективну маршрутизацію, але для попереднього дослідження маршрутів потрібно початковий потік запитів.

4.2. Ліквідація надмірності додатків за допомогою локальної обробки з використанням спрямованої дифузії з мобільними агентами

Як було сказано вище, з урахуванням специфіки додатків сенсорних мереж, датчик повинен мати різні можливості для роботи з декількома додатками. Однак для вбудованого вузла з обмеженою пам'яттю нереально зберігати в локальній пам'яті всі можливі коди програм. Введення МА не тільки забезпечує ефективний спосіб динамічної розгортки нових додатків, але також дозволяє вузлу-джерелу проводити локальну обробку «сирих» даних, коли програма. Ця можливість дозволяє зменшити кількість переданих даних, оскільки тільки релевантна інформація буде виділена і передана. Таким чином розмір стиснених даних можна представити у вигляді:

$$R_i = S_d^i (1 - r) \qquad (4.1)$$

R_i – розмір стиснених даних;

S_d^i – розмір блоку вихідних даних на вузлі i

r (0 <r <1) – коефіцієнт стиснення даних з використанням локальної обробки за допомогою МА;

Ступінь кореляції прийнятих даних між сенсорами сильно залежить від відстані між сенсорами, так що дуже ймовірно, що близько розташовані сенсори будуть видавати надлишкові дані. Таким чином, агрегація даних, що ліквідує передачу непотрібних даних, є важливою функцією в мережі з щільним розміщенням сенсорів. Основною перевагою її є усунення надмірності і, як наслідок, продовження часу життя мережі.

Порядок відвідування вузлів мобільним агентом може значно позначатися на енергоспоживанні. У даній роботі алгоритм адаптований для динамічного визначення маршруту мобільним агентом.

У цьому розділі розглянемо задачу оцінки ключових параметрів продуктивності СД і СДМА, включаючи середню затримку доставки пакетів з одного кінця в інший T_{ete} і споживання енергії для відправлення пакетів даних з усіх вузлів джерел до приймального вузла (E).

Нехай T_{dd} та T_{ma} означають середню затримку доставки пакетів з одного кінця в інший для СД і СДМА відповідно. Сюди входять всі можливі затримки під час поширення даних, викликані чергами, повторною передачею через колізії в MAC, і часом передачі. Нехай H позначає кількість ретрансляційних вузлів протягом маршруту між останнім джерелом і вузлом-приймачем, який фактично є маршрутом з найменшим часом очікування серед усіх пар «джерело-приймач». Тоді середня кількість ретрансляції для всіх пар «джерело-приймач» дорівнюватиме $H+h$. S_d – розмір відправлених даних, S_h – розмір заголовка пакету. Нехай v_n – швидкість передачі даних MAC-рівні; t_{ctrl} – загальна затримка контрольних повідомлень під час успішної передачі даних. У СД паралельне відправлення кількох пакетів даних, швидше за все, може призвести до колізій в каналі, що викличе додаткову затримку передачі даних, особливо якщо кількість вузлів джерел велика. Нехай t_{acs} – середній час очікування для успішної передачі даних в СД, середній час очікування на резервному маршруті – T_r, а число пакетів даних, доставлених до вузла-приймача за час виконання завдання, – n_d. Тоді T_{dd} обчислюється за формулою:

$$T_{dd} = \frac{T_r}{n_d} + \left(\frac{S_d + S_h}{\nu_n} + t_{ctrl} + t_{acs} \right)\left(H + h\right). \qquad (4.2)$$

Якщо $n_d >> 1$, вираз (4.2) спрощується:

$$T_{dd} \approx \left(\frac{S_d + S_h}{\nu_n} + t_{ctrl} + t_{acs} \right)\left(H + h\right). \qquad (4.3)$$

У методі СДМА T_{ma} – це середній відрізок часу між часом, коли був створений МА, і часом, коли МА повертається до вузла-приймача, T_p – затримка проходження МА, T_{roam} – середній час очікування роумінгу МА; T_{back} – середня затримка проходження МА від джерела до вузла збору.

Позначимо через τ затримку доступу, S_p – розмір коду мобільного агента,що виконується; ν_p – швидкість обробки даних; нехай S_{ma}^i – розмір МА в вузлі-джерелі i; N – кількість вузлів-джерел. Тоді

$$T_{roam} = \sum_{i=1}^{N} \left(\tau + \frac{S_d}{\nu_p} + \frac{S_{ma}^i + S_p + S_h}{\nu_n} + t_{ctrl} \right). \qquad (4.4)$$

В формулі (4.4) S_{ma}^i дорівнює

$$S_{ma}^i = S_{ma}^{i-1} + S_d\left(1 - r_i\right)\left(1 - p_i\right). \qquad (4.5)$$

Нехай S^N_{ma} – розмір пакета МА, після того як МА побуває в останньому джерелі, тоді:

$$T_{back} = \left(\frac{S_{ma}^N + S_h}{\nu_n} + t_{ctrl} \right) H; \qquad (4.6)$$

$$T_{ma} = \frac{T_p}{n_d} + T_{roam} + T_{back}; \tag{4.7}$$

а при $n_d >> 1$

$$T_{ma} \approx T_{roam} + T_{back}. \tag{4.8}$$

Нехай E_{dd} і E_{ma} позначають витрату енергії для СД і СДМА відповідно. Позначимо через m_{tx} і m_{rx} споживання енергії для отримання та передачі біта відповідно. b – фіксовану витрату енергії, витраченої на передачу пакета даних, e_{ctrl} – енергія, витрачена на обмін контрольними повідомленнями для успішної передачі даних; e_{retx} – енергія, витрачена на повторну передачу у випадку колізії СД. Тоді E_{dd} дорівнює

$$E_{dd} = \left[\left(S_d + S_h \right) \left(m_{tx} + m_{rx} \right) + b + e_{ctrl} + e_{retx} \right] \left(H + h \right) N. \tag{4.9}$$

У СДМА E_p є енергією, спожитої при переміщенні МА від вузла збору до першого джерела,E_{roam} – середнє значення енергії, що споживається на роумінг МА від першого джерела до останнього; E_{back} – середнє значення енергії, спожитої при проходження МА від першого джерела до вузла збору даних. m_p – енергію, що витрачається на обробку одного біта. Тоді

$$E_{roam} = \sum_{i=1}^{N} \left[S_d m_p + \left(S_{ma}^i + S_p + S_h \right) \left(m_{tx} + m_{rx} \right) + b + t_{ctrl} \right]. \tag{4.10}$$

$$E_{back} = \left[\left(S_{ma}^N + S_h \right) \left(m_{tx} + m_{rx} \right) + b + t_{ctrl} \right] H. \tag{4.11}$$

$$E_{ma} = \frac{E_p}{n_d} + E_{roam} + E_{back}. \qquad (4.12)$$

Якщо число n_d набагато більше одиниці, у виразі (4.12) можна знехтувати першим доданком, а отже вираз буде мати вигляд

$$E_{ma} = E_{roam} + E_{back}.$$

Наведені формули використовуються для порівняльного аналізу характеристик затримки та енергоспоживання при застосуванні методів СД і СДМА. На (рис. 4.1) та (рис.4.2) зображені графіки середньої розсіяної енергії (у відсотках на вузол) і середньої затримки доставки в секундах в залежності від числа n_d пакетів, що пересилаються, в секунду. СД - метод спрямованої дифузії, МА - комбінація методу СД з технологією мобільних агентів.

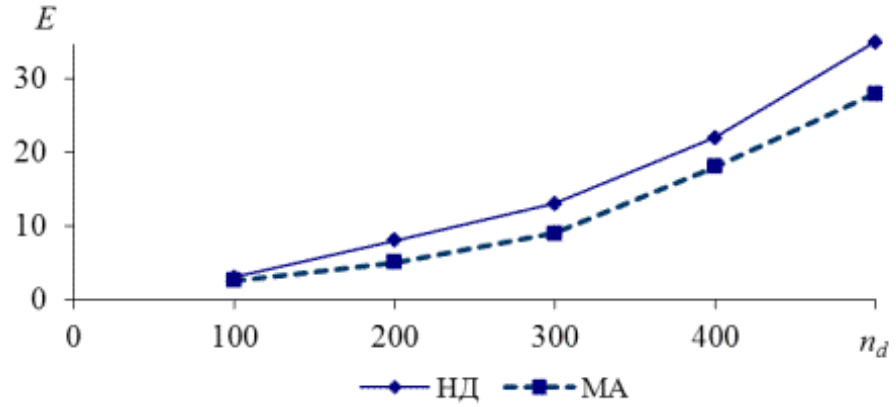

Рис. 4.1. Залежність середньої розсіяної енергії (у відсотках на вузол) від n_d

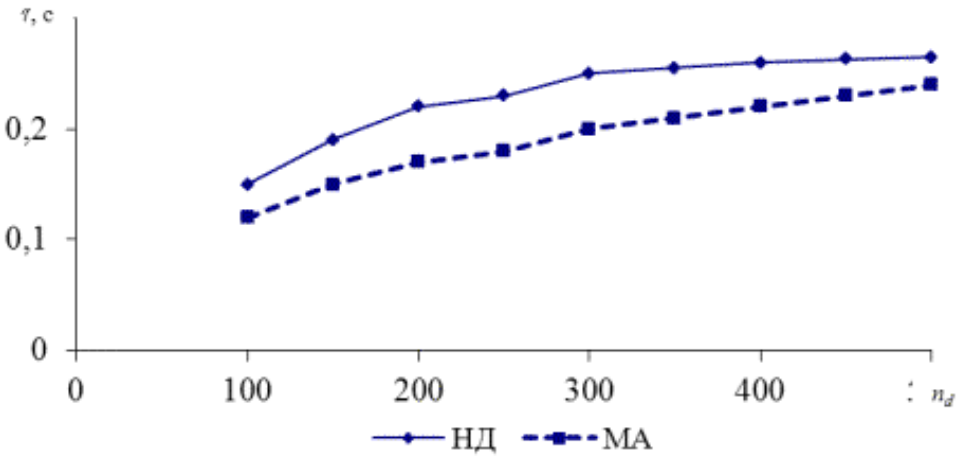

Рис. 4.2. Залежність середньої затримки доставки від n_d

При проведенні розрахунків і моделювання на ЕОМ за формулами (4.7) та (4.12) встановлено, що в 70% випадків метод СДМА дає затримку доставки приблизно на 15% - 25% менше, ніж метод СД. Перевищення затримки доставки даних при використанні методу СДМА в порівнянні з методом СД не спостерігалося. Відповідно, і витрату енергії при використанні методу СДМА у всіх випадках не вище, ніж за методом звичайної спрямованої дифузії.

4.3. Балансування навантаження при багатошляховій маршрутизації

Алгоритм маршрутизації реалізується тією частиною програмного забезпечення мережного рівня, яка відповідає за вибір вихідний лінії для відправки пакету, який прийшов. Такі цілі алгоритмів маршрутизації, як справедливість і ефективність, можуть здатися очевидними – навряд чи хто-небудь стане заперечувати проти них, – однак вони часто виявляються взаємовиключними. Очевидно, необхідний компроміс між справедливим виділенням трафіку всім станціям і оптимальним використанням каналу в глобальному сенсі. Перш ніж намагатися шукати прийнятне співвідношення справедливості та оптимальності, слід вирішити, що саме треба оптимізувати.

Можна мінімізувати середній час затримки або збільшити пропускну здатність мережі. Однак ці цілі також суперечать один одному, оскільки робота будь-якої системи з чергами поблизу максимуму продуктивності передбачає довге

стояння в чергах. Як компроміс багато мереж намагаються мінімізувати кількість пересилань для кожного пакета, оскільки при цьому знижується час проходження пакета по мережі, а також знижується навантаження на мережу, в результаті чого поліпшується пропускна здатність.

Розв’язання конфлікту справедливості та оптимальності у процесі маршрутизації тісно пов’язане з балансом потоків для мережі з необмеженою пам'яттю у вузлах.

Розглянемо мережу, що складається з *W* вузлів комутації пакетів, пам'ять яких являє собою пул однорідних буферів. Канали зв'язку для простоти передбачаються абсолютно надійними, так що повторення передачі пакетів між сусідніми вузлами визначається лише зайнятістю буферної пам'яті вузла. Пакети надходять у мережу з *R* зовнішніх джерел з інтенсивністю $\Lambda_r = (r = \overline{1,R})$.

Нехай $\lambda_{0i}(r) = \Lambda_r P_{0i}(r)$. Тоді очевидно, що загальний потік, що надходить у мережу, $\Lambda = \sum_{r=1}^{R}\sum_{i=1}^{W}\lambda_{0i}(r)$.

Рівняння балансу потоків для вузлів розглянутої мережі має вигляд

$$\begin{aligned}&\lambda_i(r) = \lambda_{0i}(r) + \sum\nolimits_{R=1}^{W}\lambda_R(r)\pi_R(\lambda_R)P_{Ri} + \\ &+\lambda_i(r)(1-\pi_i(\lambda_i)),\ i=\overline{1,W};\ r=\overline{1,R},\end{aligned} \tag{4.13}$$

де $\lambda_R = \sum_{R=1}^{W}\lambda_R(r); \pi_R(\lambda_R)$ - стаціонарна імовірність наявності вільного буфера в R-му вузлі мережі.

Система (13) може бути записана у виді

$$\lambda_i(r) = \frac{1}{\pi_i(r)}(\lambda_{0i}(r) + \sum\lambda_R(r)\pi_R(\lambda_R(r)P_{Ri}(r)). \tag{4.14}$$

Вводячи позначення $\gamma_i(r) = \lambda_i(r)\pi_i(\lambda_i), i=\overline{1,W}; r=\overline{1,R},$ і підставляючи $\gamma_i(r)$ в (2), одержуємо систему рівнянь балансу потоків для мережі з необмеженою пам'яттю у вузлах

$$\gamma_i(r) = \lambda_{0i}(r) + \sum_{R=1}^{W}\gamma_R P_{Ri}(r) \tag{4.15}$$

Останнє вираження показує, що, зберігаючи баланс потоків, що пропускаються мережею, інтенсивності потоків у вузли з обмеженою буферною пам'яттю перевершують відповідну інтенсивність мережі з необмеженою пам'яттю в $1/\pi_i(\lambda_i)$ разів . При цьому число повторень передачі по каналах мережі $(R,i)R \neq i; R,i = \overline{1,W}$ можна вважати розподіленим по геометричному закону із середнім $1/\pi(\lambda_i)$. Останнє еквівалентно збільшенню відносної частоти відвідування центрів обслуговування моделі замкнутої мережі МО при F_i=1-$\pi_i(\lambda_i)$. Таким чином, взаємовплив при міжвузловому квітіруванні виявляється у функціональній залежності

$$\pi_i(\lambda_i) = \Phi_i(\pi_i(\lambda_i),.....,\pi_W(\lambda_W)). \qquad (4.16)$$

Для прийняття рішення про маршрутизацію пакетів по критерію рівномірного завантаження мережі слід використовувати інформацію про топологію мережі та стан завантаження шляху від активного маршрутизатора до вузла призначення пакетів. Найбільш раціональним є варіант використання пакетів даних для визначення затримок до тих вузлів шлях до яких відомий активному маршрутизатору. Для визначення затримок у тій частині мережі, топологія якої невідома використовувати службові команди серверів. Теоретично можливо використати запропонований підхід для прийняття рішення про маршрутизацію пакетів в мережі на стеці протоколів TCP/IP.

Результати розрахунків і моделювання показують, що результуюча затримка при використанні СД-МА в рідкісних випадках гірше, ніж у СД, але в більшості випадків енергоспоживання СД-МА менше. Таким чином, для застосувань, де споживання енергії має першорядне значення, СД-МА дозволяє значно продовжити життєвий цикл мережі, ніж звичайна СД.

Запропонована методика дозволяє знизити завантаженість мережі та запобігти перевантаженню її окремих ланок. Існуючі технічні рішення дозволяють побудувати систему без обов’язкового впровадження програмного забезпечення, створеного на основі запропонованої методики, на сусідні для

активного маршрутизатора.

ВИСНОВКИ ДО РОЗДІЛУ 4

У даному розділі була проведена робота по оптимізації сенсорної мережі для подальшого її використання у практичних цілях для побудови автоматизованої системи на прикладі готелю.

Другий та третій підрозділи містять у собі розрахунки ліквідації надмірності додатків за допомогою локальної обробки з використанням спрямованої дифузії з мобільними агентами і балансування навантаження при багатошляховій маршрутизації відповідно. У першому підрозділі розгорнуто наведено постановку задачі.

Розроблені методики дозволяють створити механізм зменшення навантаження на окремі ланки мережі за рахунок балансування пакетів при прийнятті рішення про маршрутизацію.

РОЗДІЛ 5

АВТОМАТИЗАЦІЯ ЗА ДОПОМОГОЮ СЕНСОРНОЇ МЕРЕЖІ

Сьогодні, сучасні технології дають нам величезні можливості для створення різноманітних мереж для різних цілей, конфігурації і складності. Bluetooth технологія не є винятком. Цю технологію ми можемо використовувати для створення цілої системи. Це дасть змогу реалізувати велику кількість послуг. Така система передбачає використання для реєстрації, обробки і контролю телеметричної інформації від розподілених об'єктів за відсутності з'єднання кабелю і додаткового джерела енергії керованих об'єктів (у нашому випадку - контроль датчиків).

Завданням на планування є дослідження поняття сенсорної мережі, розгляд проблем, пов’язаних з труднощами організації мережі, з метою подальшої реалізації «розумної» сенсорної мережі на прикладі автоматизації готелю. Під автоматизацією слід розуміти наступне: кожен споживач зможе самостійно замовити або навіть налаштувати параметри, такі як опалення, освітлення, кондиціювання повітря та ін., своїх апартаментів під свої особисті потреби.

5.1. Функції системи

1. Первинні:
   - вимірювання технологічних параметрів;
   - збір даних;
   - обробка даних;
   - візуалізація збереженої інформації;
   - забезпечення взаємодії "людина - машина".

2. Вторинні:

- регулювання каналів датчиків;
- набір і керування мережею у своїх робочих режимах;
- управління режимами одного радіо ресурсу.

5.2. Основне обладнання та переваги

До основаного обладнання відносяться:

- сенсорні вимірювальні модулі, які містять у своєму складі, датчиків фізичних величин і передачі даних по безпроводовій мережі (Bluetooth модуль);
- комунікаційні модулі, які діють як маршрутизатори і ретранслятори;
- базова станція, яка є центральним вузлом мережі радіозв'язку;
- автоматизоване робоче місце для збору, зберігання і обробки отриманої інформації (сервер).

Переваги:

- не потребує кабелю зв'язку;
- можливість трансформації чутливості і режимів роботи датчиків;
- простота і низькі витрати на технічне обслуговування;
- сумісність зі стандартними і спеціалізованими платформами та програмним забезпеченням.

Як приклад такої системи, буде розроблений план автоматизації готелю. На практиці ми зустрічаємося з деякими проблемами: з відсутністю готових пристроїв, таким чином можна впровадити два можливі варіанти реалізацію мережі. Основні параметри контролю опалення, освітлення кімнати, вікна механізмів управління та контролю кондиціонерів.

5.3. Практичне застосування

5.3.1. Перший варіант реалізації

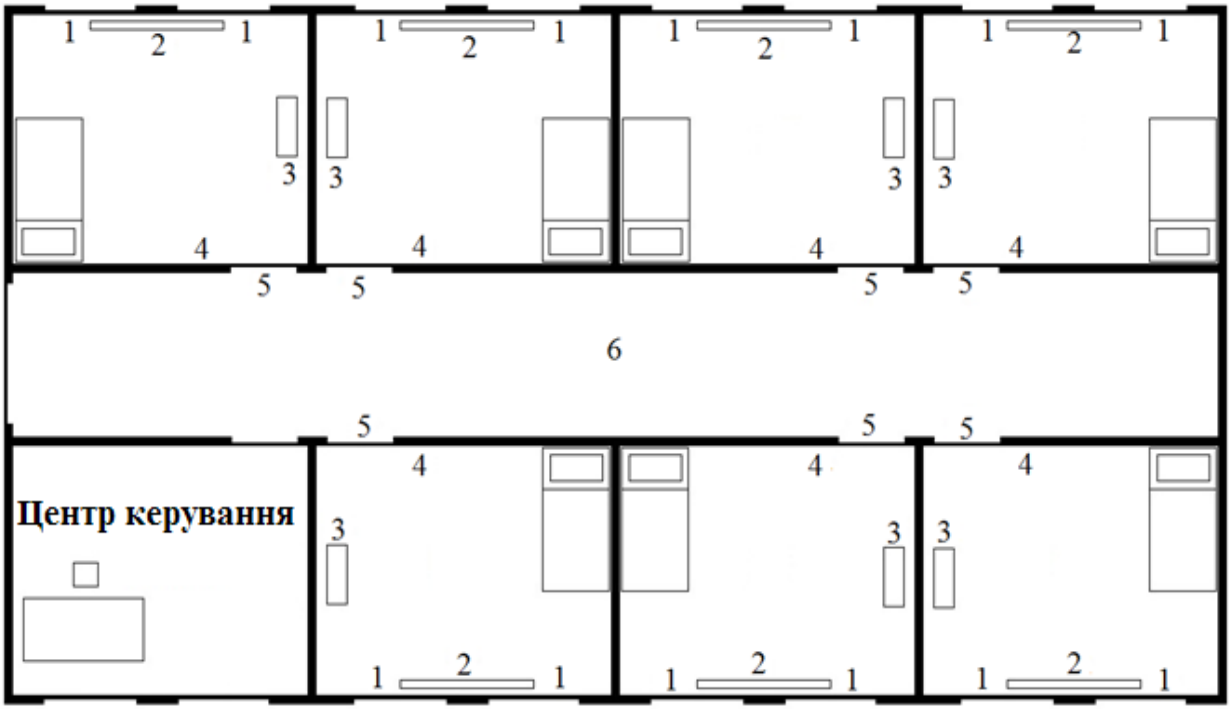

Рис. 5.1. План мережі: 1 – сенсор контролю вікна; 2 – сенсор опалення; 3 – сенсор на кондиціонері; 4 – блок освітлення; 5 – Bluetooth маршрутизатор; 6 – Bluetooth-сервер.

У цьому випадку ми будемо використовувати тільки Bluetooth-сервер, який буде керувати мережею з семи Bluetooth-маршрутизаторів. Кожен маршрутизатор Bluetooth пов'язаний з його об'єктом, в даному випадку з кількістю сенсорів у кімнаті. Інші сервера Bluetooth зв'язується з диспетчерською (або серверною) через Wi-Fi. Bluetooth-сервер дозволяє одночасне підключення 28 пристроїв, так що якщо буде потреба у розширенні мережі, не повинно виникнути жодних проблем. Складність полягає в тому, що в даний час проходить розробка пристрою, який може виступати в якості посередника між сервером і Bluetooth-сенсором, тобто ретранслятора.

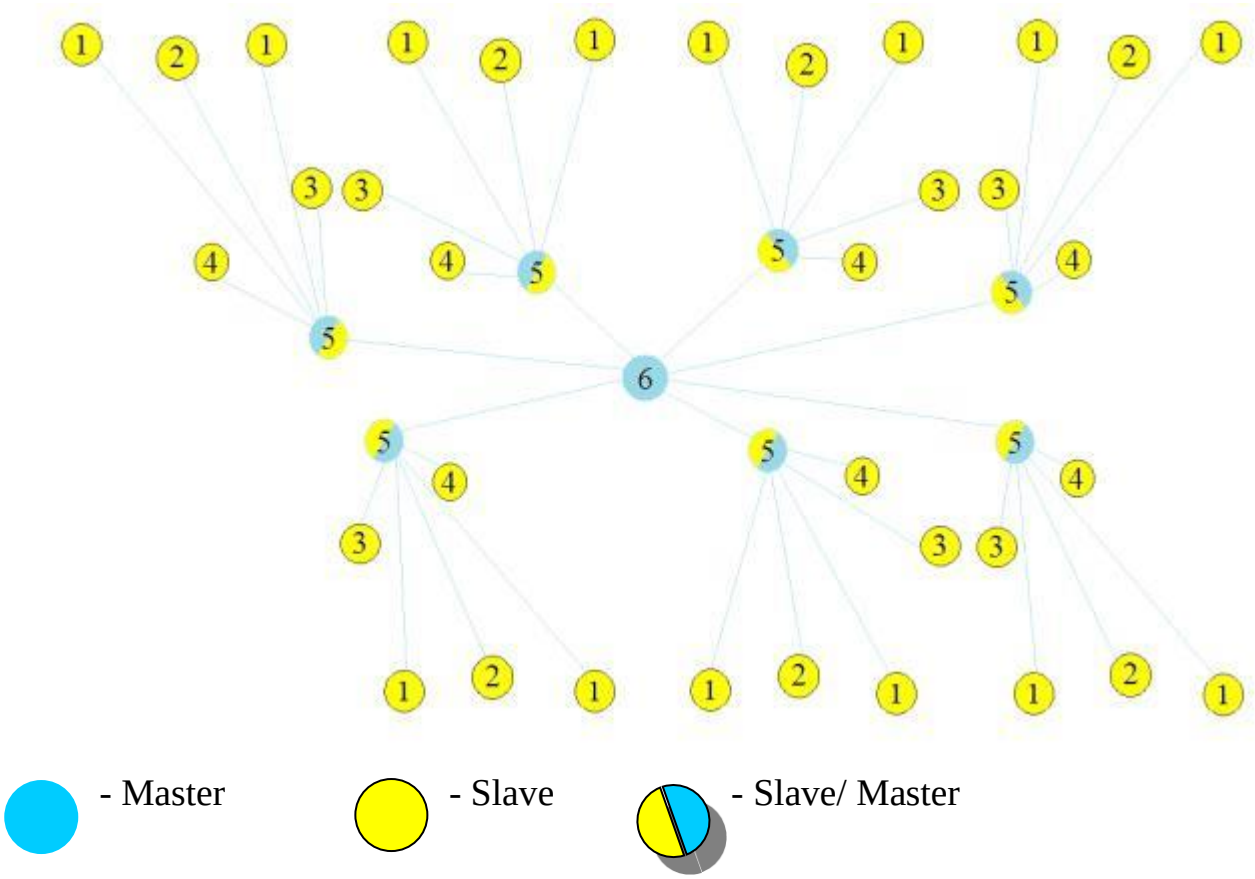

Рис. 5.2. Bluetooth ScatterNet

5.3.2. Другий варіант реалізації

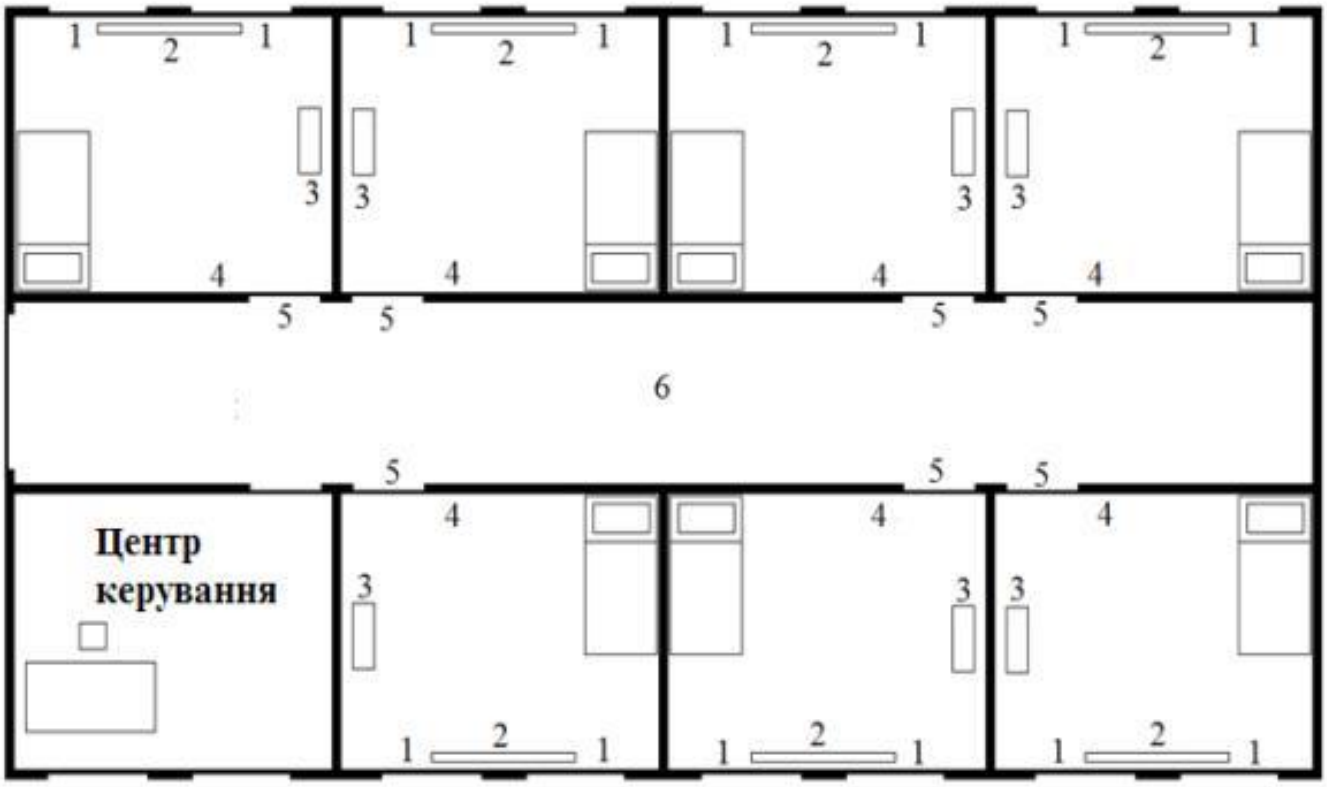

Рис. 5.3. Мережа з Wi-Fi маршрутизатором: 1 – сенсор контролю вікна; 2 – сенсор опалення; 3 – сенсор на кондиціонері; 4 – блок освітлення; 5 – точка доступу Bluetooth (шлюз); 6 – Wi-Fi роутер.

Цей варіант є більш зручним, але і дорожчим. Ми будемо відмовлятися від створення Bluetooth ретранслятора і використовувати точки доступу Bluetooth у якості проміжного пристрою. Передача інформації від датчиків підходить для Bluetooth-точку доступу, пов'язані з встановленим на поверсі Wi-Fi маршрутизатором. У свою чергу, Wi-Fi маршрутизатор посилає збереження інформації на сервер. Проблема цього методу є додатковим джерелом енергії для кожної точки доступу Bluetooth і Wi-Fi маршрутизаторів.

Таблиця 5.1. Порівняння спроектованих мереж

Параметри	Перший план	Другий план
Принцип реалізації	Один сервер Bluetooth повністю контролює усіма сенсорами на поверсі за допомогою спеціального маршрутизатор Bluetooth.	Один Wi-Fi маршрутизатор контролює поверх через точку доступу Blutooth (в кожній кімнаті власна точка доступу)
Переваги	1) потрібно менше додаткового обладнання; 2) ніяких додаткових джерел енергії; 3) простота зв'язку між поверхами.	1) відсутність складної Scatternet (Звичайна пікомережа); 2) прямий зв'язок між сервером і сенсорами.
Недоліки	1) Потреби розробки маршрутизатора Bluetooth; 2) складність мережі. 3) доволі посередня якість сигналу 4) велика вартість	1) для кожного пристрою (Wi-Fi маршрутизатори, точки доступу Bluetooth); 2) труднощі з подальшим розширенням.

ВИСНОВКИ ДО РОЗДІЛУ 5

Даний завершальний розділ був присвячений практичному застосуванню та реалізації безповодової MESH-системи побудованої на основі сенсорних датчиків.

Дивлячись на тенденцію укорінення технологій в життя людини, постійний розвиток та автоматизацію величезної кількості сфер діяльності людства, неодмінно потрібна адаптація та налаштування високих технологій під своєрідні та незвичайні потреби людства.

Отже можна зробити висновок, що даний проект може знайти широке застосування у майбутньому, оскільки така система дасть можливість зменшити втручання людського ресурсу у робочий процес. Мережа такого плану можлива для реалізації не тільки в готелі, така система прийнятна і для лікарень, портів, шкіл або будь-яких інших установ.

ОСНОВНІ РЕЗУЛЬТАТИ ТА ВИСНОВКИ

Сучасні досягнення мікроелектроніки дозволяють інтегрувати на одному крихітному кремнієвому кристалі як обчислювальні блоки, так і всі необхідні пристрої для підтримки безпроводових мереж – глобальних, локальних і персональних. А якщо на цьому ж кристалі розташувати й пристрої для передачі даних, голосу та відео? Вже можливо створювати радіопристрої, здатні працювати в декількох режимах і в різних мережах одночасно (наприклад, «інтелектуальні» мобільні телефони і комунікатори). І скоро все це буде зосереджене на одному кристалі, який можна розмістити в наручних годиннику, в мініатюрних навушниках, мікрофоні, нагрудному значку і так далі. Причому всі ці «чудеса» стануть доступні розробникам додатків і споживачам вже наприкінці поточного десятиліття, а то і раніше.

Можливості застосувати «мініатюрне напівпровідникове радіо» обмежені тільки нашої фантазією. Можна організувати сенсорне середовище з використанням функцій безпроводової передачі даних, наприклад, для температурного або хімічного аналізу. А оскільки вартість таких датчиків складе кілька центів або навіть частку цента, то легко інтегрувати подібні обчислювальні пристрої прямо в навколишнє середовище.

Вкрай багатообіцяюче застосування сенсорів у медицині - моніторинг серцевого ритму, вимірювання кров'яного тиску і ряду інших життєво важливих показників для автоматичного попередження лікарів і надання, у разі потреби, невідкладної допомоги, полегшення життя хворим і людям похилого віку, поліпшення комфортності у звичайному житті. Обладнане різноманітними сенсорами дитяче ліжечко здатне не тільки контролювати дихання дитини і уловлювати зміни температури його тіла, а й попереджати дорослих про небезпечні зміни або навіть самостійно вживати якихось заходів. А плавальний басейн може самостійно контролювати свіжість і чистоту води ...

Можливості використання сенсорних MESH- мереж простягаються далеко за межі будинку, офісу або медичного закладу - експерти називають, насамперед,

екологію та служби порятунку: малесенькі датчики, розкидані з літаків над великими лісовими масивами можуть відслідковувати виникнення лісових пожеж, або маршрут заблукавшої туристичної групи, передаючи в диспетчерський центр з самоорганізованої безпроводової мережі доскональний моніторинг стану «зеленого океану». Вони ж можуть стежити за дозріванням урожаю, інформуючи фермерів, коли не вистачає вологи або добрив і так далі.

В ході роботе виконаний порівняльний аналіз мереж радіодатчиків, що працюють по алгоритму мобільних агентів, и мереж, в яких застосовується алгоритм мобільних агентів з спрямованою дифузією потоків даних від вузлів-джерел до вузлів-приймачів. Результати розрахунків та моделювання показують, що результуюча затримка при використанні СДМА лише в деяких випадках гірша, ніж у СД, але у більшості випадків енергоспоживання СДМА менше. Таким чином, для застосування, де споживання енергії має першочергове значення, СДМА дозволяє значно подовжити життєвий цикл мережі, ніж звичайна СД.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. L. Buttyan, J.-P. Hubaux. Security and Cooperation in Wireless Networks.Cambridge University Press, 2007. – 496 p.

2. L. Buttyan, V. Gligor, D. Westhoff. Security and Privacy in Ad Hoc and Sensor Networks. Lecture Notes in Computer Science No. 4357. – Springer, 2007. – 193c.

3. Гладиш С. В. Реактивні технології безпеки безпроводових мереж // X Міжнародна науково-практична конференція "Безпека інформації в інформаційно-телекомунікаційних системах". - 20 - 23 травня 2008. – Пуща Озерна, Київ. - с. 102 – 103

4. Chalermek Intanagonwiwat, Ramesh Govindan, and Deborah Estrin. Directed diffusion: a scalable and robust communication paradigm for sensor networks. Proceedings of the 6th annual international confer-ence on Mobile computing and networking, Boston, Massachusetts, United States, pages 56 – 67, 2000.

5. Diona Bein, Ajoy K. Datta. A Self-Stabilizing Directed Diffusion Protocol for Sensor Networks. International Conference on Parallel Processing Workshops, Montreal, Quebec, Canada, August 15-August 18 2004.

6. Андрій Зубинський. Распыленная разумность. Компьютерное обозрение №8 26 лютого - 4 березня 2003.

7. Алекс Карабуто. Сенсорные сети: как скоро?. Комп’ютерра, 25 серпня 2004.

8. CC1100 Single-Chip Low Cost Low Power RF-Transceiver (Rev. D). SWRS038D. Chipcon Products from Texas Instruments, 25 May 2009.

9. Бройдо В.Л. Вичислительные системи, сети и телекоммуникации. Учебник для ВУЗов.2е издание. – СПб.: Питер, 2004. - 703 с.

10. Джим Гейер. Беспроводные сети. Первый шаг: Перевод с англ. – М.: Издательский дом «Вильяме», 2005.- 192 с.

11. Э. Танненбаум. Компьютерные сети. 4е издание. – СПб.: 2003.- 992 с.

12. В.М. Вишневский, А.И. Ляхов, С.Л. Портной, И.В. Шахнович. Широкосмуговые беспроводные сети передачи информации. – М.: Техносфера, 2005. – 592 с.

13. В.Г. Олифер, Н.А.Олифер. Компьютерные сети. Принципы, технологии, протоколы: Учебник для ВУЗов. 4е издание. – СПб.: Питер, 2010. – 944 с.